U.S. v. Ross Ulbricht, S1 14 Cr. 68 (KBF)
Howard, Timothy (USANYS) 1
to:
forrestnysdchambers@nysd.uscourts.gov
05/19/2015 03:01 PM
Cc:
"Turner, Serrin (USANYS)", "jdratel@joshuadratel.com", Lindsay Lewis
Hide Details
From: "Howard, Timothy (USANYS) 1" <Timothy.Howard@usdoj.gov>

14 cr 68 (KBF)

To: "forrestnysdchambers@nysd.uscourts.gov" <forrestnysdchambers@nysd.uscourts.gov>

Cc: "Turner, Serrin (USANYS)" <Serrin.Turner@usdoj.gov>, "jdratel@joshuadratel.com" <jdratel@joshuadratel.com>, Lindsay Lewis <LLewis@joshuadratel.com>

1 Attachment

Criminology and Criminal Justice-2014-Martin-3.pdf

Dear Judge Forrest,

Attached please find a copy of the article requested in paragraph 6(b) of the Court's Order from earlier today, courtesy of defense counsel.

The Parties do not have a copy of the book referenced in paragraph 6(a) of the same Order.

Respectfully,
Tim Howard

ordered
Pass to docket.
KB. Forrest
USDJ
5/20/15

Timothy T. Howard
Assistant United States Attorney
United States Attorney's Office, Southern District of New York
Complex Frauds and Cybercrime Unit

One St. Andrew's Plaza

New York, NY 10007
Tel: 212.637.2308
Fax: 212.637.2429
timothy.howard@usdoj.gov

Criminology and Criminal Justice
http://crj.sagepub.com/

Lost on the *Silk Road*: Online drug distribution and the 'cryptomarket'

James Martin

Criminology and Criminal Justice 2014 14: 351 originally published online 7 October 2013
DOI: 10.1177/1748895813505234

The online version of this article can be found at:
http://crj.sagepub.com/content/14/3/351

Published by:
SAGE
http://www.sagepublications.com

On behalf of:
BSC
British Society of Criminology

>> Version of Record - Jun 19, 2014

OnlineFirst Version of Record - Oct 7, 2013

Article

Criminology & Criminal Justice
2014, Vol. 14(3) 351–367

DOI: 10.1177/1748895813505234
crj.sagepub.com
SAGE

Lost on the *Silk Road*: Online drug distribution and the 'cryptomarket'

James Martin
Macquarie University, Australia

Abstract

The illicit drugs website, *Silk Road*, presents an ideal case study for how online communication technologies are transforming crime. This article seeks to locate the offences committed via *Silk Road* within existing cybercrime literature, and presents a new criminological concept – the cryptomarket – to outline the contours of this new generation of online illicit marketplace. Cryptomarkets are defined as a type of website that employs advanced encryption to protect the anonymity of users. The article also analyses the implications *Silk Road* has for drug consumers and law enforcement, as well as the potential changes to drug distribution networks that are likely to occur if *Silk Road* and other cryptomarkets continue to assume a greater share of the global trade in illicit drugs. In conclusion, it is argued that while *Silk Road* presents a less violent alternative to conventional drug distribution networks, the risks posed by the rapid proliferation of cryptomarkets more generally are largely unknown and require further research.

Keywords

Cybercrime, cryptomarket, drug distribution networks, *Silk Road* (website), War on Drugs

Introduction

This article explores the continuing rise of *Silk Road*, a website which facilitates the sale of illicit drugs and operates on the TOR network,[1] an encrypted part of the internet otherwise known as the 'dark net'. The article has two related aims: the first seeks to locate the offences associated with *Silk Road* within the realm of cybercrime. A background section outlines the empirical dimensions of the site and describes the operational format and recent growth statistics (for a more detailed discussion of this – see Christin, 2012).

Corresponding author:
James Martin, Centre for Policing, Intelligence and Counter-terrorism, Macquarie University, Australia.
Email: james.martin@mq.edu.au

Existing cybercrime typologies are then analysed with reference to *Silk Road*, and to the operation of other online illicit marketplaces (OIMs). At present, existing cybercrime typologies do not appear to reflect adequately the complexity associated with *Silk Road* and other novel forms of online illicit exchange. This is because existing typologies tend to categorize cybercrimes in isolation as singular acts rather than involving the commission of numerous offences linked by a common purpose. The multi-stage nature of online drug distribution that is associated with *Silk Road*, which involves the commission of both online and offline offences, challenges these perspectives. The limitations associated with existing cybercrime typologies are examined in depth and a new cybercrime concept – the cryptomarket – is proposed. This provides an ideal type for scholarly consideration, as well as outlining an emerging area of cybercrime for further research.

The second aim is to explore the immediate and long-term implications of the development of *Silk Road*. Seller pages hosted on the site were accessed by the researcher and are presented to demonstrate the types of services now available. These help illustrate the dual role that online communications play in maintaining a high level of quality assurance and customer satisfaction, as well as in proliferating counter-interdiction strategies and smuggling techniques. The operations of *Silk Road* are then analysed with reference to conventional drug distribution networks. Existing criminological research concerning the composition of drug distribution networks is considered, and the changing relationships between drug distributors, consumers and associated law enforcement/prohibition agencies are explored. The central argument is that the changes associated with online drug distribution signal a potential paradigm shift in the global War on Drugs, as costly and ineffective prohibition strategies are placed under further stress, and new, more efficient distribution networks form between drug producers and consumers.

Background

The development of online illicit marketplaces (OIMs) is a recent phenomenon. Possibly the largest and undoubtedly one of most sophisticated of this new generation of websites, *Silk Road*, has been in operation since only 2011 (Christin, 2012: 3). *Silk Road* captured worldwide media attention following an expose in New York-based blog *Gawker* (Chen, 2011). A flurry of news articles quickly followed warning of the dangers associated with this innovative form of online illicit exchange, prompting expressions of surprise and alarm from law enforcement agencies already struggling with maintaining drug prohibition (see, for example, Moses, 2012; Ormsby, 2012; Pauli, 2012). Concern over the site has since been expressed at the highest levels of executive authority, and was notably described in the US Congress as 'the most brazen attempt to peddle drugs online we have ever seen' (Hammersly, 2012: 56). Academic interest in the site has also grown recently, with a number of scholars publishing research about different aspects of the site (see Barratt, 2012; Barratt et al., 2013; Christin, 2012; Van Hout and Bingham, 2013). The public commentary surrounding *Silk Road*, and the resultant public condemnation by law enforcement and government authorities (e.g. AFP, 2012), appear to have had little negative impact on the site. Rather, the apparent inability to close *Silk Road* down may have served only to further embolden new and existing users and stimulate further online illicit exchange.

Silk Road differs from conventional forms of illicit exchange by being facilitated through the internet. Buyers and sellers use advanced digital encryption to log on to the site anonymously. They then buy and sell all manner of legal, controlled and prohibited narcotics. The site is facilitated by a third party administrator who appropriates a percentage of each sale conducted. Transactions are completed using Bitcoin, an encrypted e-currency (Nakamoto, 2008), and purchased goods are then posted directly by the seller to a recipient address. Buyers, sellers and facilitators need never reveal their true identities, meet face-to-face, nor even be in the same country. This offers users the significant benefit of reducing the possibility of violence associated with 'in-person' forms of illicit exchange. Upon receipt of an order, buyers provide a satisfaction rating (out of five stars) and offer any comments for consideration, providing others contemplating similar purchases with important information about the quality of goods received and the reliability of the supplier (Christin, 2012). These user-friendly features, together with the ease and relative safety of the online exchange hosted by *Silk Road*, have led commentators to make direct comparisons with legitimate internet marketplaces, often referring to the site as the 'eBay of illicit drugs' (Ormsby, 2012; Pauli, 2012).

At the present time, the apparently modest scale of online illicit exchange appears little cause for alarm, particularly when compared to the scale of conventional illicit drug distribution. For example, in 2005, the United Nations Office on Drugs and Crime estimated the annual illicit drug trade in the USA to be approximately US$300 billion (UNODC, 2005) – an unreliable statistic but nevertheless representative of the type that informs policy makers and law enforcement. By contrast, the worldwide distribution of drugs facilitated through *Silk Road* is currently estimated at approximately $US23 million per year (Christin, 2012: 1). While this is a substantial sum, it is undoubtedly a tiny proportion of the overall drug market. More important, however, are the long-term upward trends: according to Christin, the number of sellers listed on the site more than doubled from 220 to over 550 in the 10 months between November 2011 and August 2012 (2012: 10); and the combined value of publicly available sales processed increased approximately 38 per cent in just six months (2012: 17). If the current growth of turnover is maintained, it seems reasonable to assume that the value of publicly listed transactions traded through *Silk Road* will approach $US60 million by the end of 2013. These trends suggests that while the overall proportion of illicit drugs currently channelled through *Silk Road* is comparatively small, this will not necessarily remain the case for long.

Conceptualization – *Silk Road* as Cybercrime

Given that *Silk Road* drug distribution networks are facilitated through the internet, a logical starting point in terms of conceptualization is within the realm of cybercrime. Despite being a relatively new area of criminology, various scholars have established a range of typologies to assist in analysing computer-related offences. Jewkes and Yar (2010: 3), for example, note the well-established dichotomy between 'computer-assisted' and 'computer-oriented' or 'computer focused' cybercrimes, with the former relating to offences that exist independently of the online world but are now augmented or

facilitated through the use of computers, while the latter are both unique to and entirely dependent upon the internet and associated technologies. Examples of 'traditional' sorts of offences that have been reinvented as computer-assisted cybercrimes include fraud, theft and defamation. Computer-focused cybercrimes, on the other hand, necessarily involve the use of online technologies, and examples include computer hacking, the creation of malicious software (viruses, worms, Trojans, etc.) and the hijacking or 'enslaving' of infected computers (Jewkes and Yar, 2010).

Due to the fact that OIMs such as *Silk Road* facilitate forms of offending (i.e. the sale and distribution of illicit goods) that are long established and clearly predate the development of the internet, it seems logical to classify these activities as computer-assisted rather than computer-oriented. However, when considering this classification in further depth, the foundational dichotomy between computer-assisted and -focused cybercrimes begins to break down. One of the reasons for this is that *Silk Road* employs a multi-stage process that involves a broad range of novel and conventional offences that are dependent upon computer technology to widely varying degrees. Particularly, *Silk Road* transactions are dependent upon the anonymity provided by advanced encryption technologies, as well as the capacity for sellers to access simultaneously massive numbers of users online. This dependency on the internet and computer systems to access user networks and conduct online illicit transactions suggests that these aspects of *Silk Road* operation are more closely aligned with computer-focused rather than computer-assisted cybercrimes. The initial, highly sophisticated and encrypted stages of online exchange contrast significantly, however, with subsequent processes. Once orders facilitated through *Silk Road* are finalized, the distribution and trafficking of illicit goods takes place using effectively no computer technology; goods are simply packaged and transported through traditional postal systems. This contrastingly 'low tech' approach means that some of the most serious offences associated with the site (i.e. the trafficking of illicit goods across national borders), are not, in fact, cybercrimes at all. Rather they represent offences that are qualitatively no different from conventional forms of smuggling.

Wall (2007) acknowledges the deficiencies of the simple binary classification of computer-oriented and -focused cybercrimes, and instead proposes a 'transformation test' that assesses computer-related offences according to their integration with online networks. Describing the purpose of the transformation test, and the critical relationship between networks and cybercrime, Wall (2007: 34) notes that:

> Because the defining characteristic of cybercrime is its mediation by networked technologies, the test of a cybercrime must focus upon what is left if those same networked technologies are removed from the equation … The particular transformations that affect the digital architecture of criminal opportunity are … the growth in networking through the convergence of technologies, the importance of informational transfer and brokering … and globalisation. These transformations are not simply the product of technology … rather they signify broader processes and provide useful focal points.

Wall's transformation test categorizes cybercrimes into various generations, two of which are relevant to *Silk Road*. First-generation cybercrimes are those that are facilitated by computers operating within closed or discrete network systems. For example,

breaking into a bank and using a computer to disable its internal alarm system would constitute a first-generation cybercrime; no external network of computers has been exploited or disrupted in the commission of the offence. First-generation cybercrimes are similar to 'computer-assisted' offences in that they persist independently of broader networks; if one 'transforms' the offence by hypothetically eliminating the involvement of computers and online networks, then criminal 'activities will persist by other means' (Wall, 2007: 45).

Second-generation cybercrimes, by contrast, involve the exploitation of the vast illicit opportunities provided by global information networks. If one hypothesizes transformation by removing computers and associated online networks, then second-generation offences may still continue but only at a significantly reduced rate (Wall, 2007: 46–47). An example of second-generation cybercrime is the distribution of prohibited images over the internet. Offenders who share images of child pornography online may still exchange these offline and in-person, but are presumably much less likely to do so; the commission of this type of offence is therefore dependent to a large extent upon the existence of large networks that may only be accessed through computerized and networked communications technology.

The operations of *Silk Road* generally fall under this second-generation classification. If the presence of online networks is hypothetically removed then undoubtedly the distribution of illicit goods will persist by other means. Even with this more sophisticated cybercrime typology, however, problems emerge when attempting to conceptualize the activities of OIMs. Just as is the case with the binary 'computer-assisted' versus 'computer-oriented' model described by Jewkes and Yar (2010), OIMs are difficult to place within any one category; instead they share characteristics with multiple generations of cybercrime. With regards to categorizing OIMs as first-generation cybercrimes, the sale and distribution of illicit goods has throughout history as well as in the present day often been undertaken without the use of computers or associated network technologies. This suggests that the operations associated with OIMs are first-generation cybercrimes. Significantly, Wall (2007: 45) also offers specific commentary on this point, noting that the online activities of drug dealers constitute first-generation cybercrimes.

Importantly, however, *online* sales and distribution of illicit goods are, naturally, dependent upon computer networks. Without online communications to facilitate this process, the illicit distribution networks of the type presented by *Silk Road* would not exist. Instead, transnational drug distribution would take place as it did in the pre-internet era, that is, large-scale drug supplies would still be maintained, but would be distributed through complex criminal networks, with a reliance on multiple layers of importers, wholesalers and street-level dealers (Pearson and Hobbs, 2001; Ruggerio, 2000). The illicit exchanges conducted through *Silk Road*, while ostensibly involving the conventional offences of sale and trafficking of illicit goods, are reliant on online distribution networks that are qualitatively different from those associated with traditional, offline illicit exchange. In the same way that the global operations of eBay and Amazon market differ significantly from local trading marketplaces, so too do the operations of *Silk Road* differ from those of traditional drug distributors and street dealers. This difference is not adequately reflected in existing cybercrime typologies. This suggests the need for a new

form of conceptualization to capture the particular features inherent to *Silk Road* and other similar OIMs.

Online Illicit Marketplaces and the Cryptomarket

Given the limitations apparent to conceptualizing *Silk Road* as cybercrime, it may be more useful to view it rather as a specific type of OIM, particularly a cryptomarket. Cryptomarket is a colloquial term that originated on internet hacker forums. The purpose of this section is to provide a scholarly definition for academic and more general usage. A cryptomarket may be defined as an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities. Because legal exchanges may be conducted in such a forum, it is not necessarily a site for the commission of cybercrime. However, the necessity or preference for users to conceal their identities points to a range of motivations, of which intention to commit crime is a significant one (other motivations may include political subversion or a commitment to privacy). The reliance on encryption technology differentiates cryptomarkets from other types of OIM, for example sites that rely on spam-marketing to sell illicit drugs from centralized locations. Ideal type cryptomarkets may also share the following characteristics:

- reliance on the TOR network;
- use of cryptonyms to conceal user identity;
- use of traditional postal systems to deliver goods;
- third-party hosting and administration;
- decentralized exchange networks;
- use of encrypted electronic currency (e.g. Bitcoin).

Silk Road is an archetypal cryptomarket. However, it is far from the only such site to be found online. A brief search through *Hidden Wikipedia* – another dark net website available through the TOR network – reveals links to more than 100 different cryptomarkets offering a range of illicit goods and services including, but not limited to: stolen credit card information; forged identity documents; plagiarized university essays; hacking/cracking services; money laundering; child pornography; illegal firearms and ammunition; and even contract killing. While it is beyond the scope of this article to investigate each of these sites, it is clear that *Silk Road* represents only the tip of a vast and rapidly proliferating body of cryptomarkets. This indicates the need for more research in this new arena of criminal activity.

Challenges to Law Enforcement

To date, state authorities have had little success in preventing the rapid proliferation of buyers and sellers populating *Silk Road* (Christin, 2012). Indeed, its continued growth suggests that law enforcement is largely failing to stem the growing volume of illicit drugs being channelled through the site. This failure is due at least in part to a host of new and complex tactical and strategic challenges facing investigators and prosecutors charged with combating online drug distribution. This section will explore the immediate

challenges that *Silk Road* poses for law enforcement, as well as some of the longer-term strategic implications for domestic drug prohibition.

Online encryption and TOR

For law enforcement agencies seeking to investigate offences committed via *Silk Road*, the immediate problem is detection. All transactions conducted through the site employ TOR encryption to mask the identity of users. This means that unless investigators monitoring the site can break the codes employed by *Silk Road*, they will be unable to learn the identities of who is either buying or selling, or where illicit goods are being sent. According to independent analysts and security experts, users of *Silk Road* have good reason to be confident that their online anonymity will go unchallenged by law enforcement. McDonald claims that policing agencies currently 'have no chance of beating [the] existing encryption' employed by *Silk Road* and other cryptomarkets operating on the TOR network (McDonald cited in Ormsby, 2012), and that authorities would need 'tens of thousands, if not millions of years to break into these algorithms' (McDonald cited in Duffy, 2012). These perspectives point to significant difficulties in 'cracking' encrypted *Silk Road* communications.

While the communications employed by users on *Silk Road* appear largely impervious to monitoring by law enforcement, the site's e-currency of choice, Bitcoin, is undoubtedly less secure. Bitcoin operates similarly to conventional, 'hard' currencies; it has a 'floated' value, meaning that the value of Bitcoin (compared to other currencies such as the US dollar or Chinese Yuan) fluctuates according to demand. Purchases of Bitcoins must be made from established, legitimate Bitcoin vendors. This purchasing stage is a point of vulnerability to detection by law enforcement. While exchanging Bitcoins for goods purchased on *Silk Road* is encrypted, transactions involving the conversion of hard currencies into Bitcoins, or vice versa, necessarily leave a trail in official financial records. This means that law enforcement agencies are able to monitor who is buying and selling Bitcoins, but remain blind as to what transactions are undertaken beyond this initial conversion stage (Blain, 2013).

The potential for exposure to law enforcement when buying and selling Bitcoins is, however, unlikely to involve significant risk for *Silk Road* users, particularly small-volume buyers. In the first instance, simply being exposed to monitoring does not necessarily mean that any such observation is taking place; authorities may lack either the awareness, resources or inclination to engage in this kind of financial monitoring. Bitcoin also has a growing number of legitimate uses (Blain, 2013), meaning that involvement in criminal activity cannot be inferred simply from trading in the e-currency. However, as authorities may be monitoring e-currency transactions, it seems likely that users would take simple, additional defensive measures, such as avoiding suspicious conversions involving large amounts of Bitcoins.

Postal inspection and buyer–seller communications

With advanced Bitcoin and TOR encryption helping to ensure the online anonymity of *Silk Road* users, the next opportunity for law enforcement to detect an offence is when

illicit goods enter and travel through the postal system. While physically inspecting postal items is more likely to result in the detection of an offence than online monitoring, this strategy is problematic on several counts. First, the rapidly expanding volume of global trade means that significantly more items are travelling through the international post than ever before. In Australia, for example, approximately 45 million postal items were sent and received internationally in 2010–2011, an increase of *56 per cent* on the previous year (Greenblat, 2011), with legitimate internet purchases fuelling much of the boom. Inspecting even a small proportion of this huge volume of mail places a significant burden on Customs resources. Customs agencies are therefore increasingly forced to narrow the focus of their limited resources towards postal items that arouse high degrees of suspicion in order to locate the proverbial needle among the haystack.

Limiting Customs inspections of items that are overtly suspicious is complicated, however, by sophisticated concealment techniques employed by sellers on *Silk Road*. Discussion forums hosted on the site offer detailed advice as to how best to avoid attracting the attention of postal and customs authorities (see Barratt et al., 2013; Schneider, 2003; and Van Hout and Bingham, 2013 for more detailed discussion of online drugs forums). These include advising sellers to vacuum seal goods and use professional looking, 'businesses style' printed envelopes (Christin, 2012: 12). Buyers are also advised to avoid ordering from countries with a reputation for exporting illicit drugs (e.g. the Netherlands or Colombia), and instead favour those which routinely attract domestic private and commercial traffic, such as the USA and Canada. Attempts at frustrating law enforcement are further assisted by the generally small quantities typical of purchases on *Silk Road* (Christin, 2012: 12). Limiting purchases to small volumes means that standard drug consignments, for example, a gram of cocaine or a '10-pack' of ecstasy, fit easily into regular (and inconspicuous) postal envelopes. This further complicates the work of Customs agents, lowers the risk of detection and likely results in fewer drugs being intercepted while in international transfer.[2]

Discussion pages hosted on *Silk Road* facilitate user collaboration in the development of a constantly updated, collective body of knowledge regarding how best to frustrate the efforts of law enforcement. In addition to providing this valuable information, the user satisfaction rating system accompanying the profile of each *Silk Road* product helps provide a systematic advantage to those sellers who adopt effective concealment methods. Each seller profile displays the vendor's ranking among all sellers on the site, as well as related statistics including how many successful transactions the seller has completed, and the number of stars out of five that they have been awarded by buyers. Higher user satisfaction ratings are associated with orders that arrive as expected, meaning that sellers who lack the necessary skills in concealment or 'stealth' are marked down by disappointed customers. This free-market mechanism ensures that more competent sellers are rewarded with increased business, and that successful concealment techniques proliferate as a result.

The user satisfaction pages and discussion forums hosted on *Silk Road* provide an insight into the quality of services offered by sellers, and the high standard expected from buyers who are able to contact literally thousands of competing drug dealers within a few

keystrokes. Consider the reviews for the seller in Figure 1, which may be interpreted as broadly representative of the more highly ranked vendors on *Silk Road*.

As the reviews in Figure 1 suggest, not only is feedback for the larger and more reliable sellers generally very positive, it is also updated with the most recent transactions, often recorded within hours of completion. This constant and up-to-date chatter is important not only for buyers who are sensitive to price changes and the quality of individual batches of narcotics. It also facilitates real-time responses to developments in law enforcement. If customs or policing agencies improve interception techniques that result in sustained increases in interceptions, up-to-date communications ensure that sellers are able to adapt quickly.

One recent example of the importance of user feedback on *Silk Road* concerned an unexpected increase in orders reportedly failing to be delivered to recipients in Australia. In response to the unfulfilled orders, buyers began complaining on discussion forums and feedback pages, and users determined that more rigorous international screening procedures had been implemented by Australian Customs. This prompted a variety of different responses from international sellers. Some chose to ban sales to Australia entirely, while others continued business as usual. More interesting were the responses from sellers who modified the 'terms and conditions' associated with purchases from Australian customers. This latter approach is exemplified by the highly ranked MDMA (ecstasy) dealers referred to in Figure 2, who recently provided this update on their seller page.

The adaptability to developments in law enforcement displayed by this seller, as well as the apparent sensitivity to buyer concerns, demonstrates the central role of user reputation in the operation of *Silk Road*. Concern over 'flaming' (i.e. hostile feedback on public forums) by disappointed Australian customers prompted this seller to reformulate their export strategy, and convey the need for lower expectations when making purchases from this particular destination. Potential buyers were quickly informed of the newly increased risks, and advised of adjustments to delivery times and changes regarding the refund policy for undelivered goods. Responsiveness of this kind of assists sellers on *Silk Road* in protecting their reputation and the profitability of their enterprise, and ensures customers have maximum information with which to make future purchasing decisions and manage the changing levels of risk posed by law enforcement.

Post-delivery challenges

It appears that online communications hosted on *Silk Road* play a crucial role in ensuring the effective concealment and quality of orders. In addition to this, online communications also provide vital information to buyers as to how best to frustrate the efforts of law enforcement in those instances when subterfuge fails and goods are intercepted. If law enforcement agencies do manage to detect a consignment of prohibited drugs, there remain significant obstacles to obtaining sufficient evidence for prosecution. Buyers using *Silk Road* are advised on discussion forums and seller Q&A pages to use pseudonyms and have goods posted to addresses other than their place of residence (e.g. a vacant house or place of business, a neighbour's residence, or a dummy post box). Goods sent to a false address can then be picked up by recipients at their leisure. Without any

Rating	review	freshness
5 of 5	Quick shipping, beautiful product, decent stealth. weighed out to 991mg, which is within the realm of error.	1 day
5 of 5	will update when tested/tasted but no reason to suspect with all the positive reviews.	1 day
5 of 5	Fast Shipping, great packaging	1 day
5 of 5	10/5 fast arrived in 4 days – double vacum sealed in stealth packaging. looks on spot – smells like licorice and very very clean!	1 day
5 of 5	A+ service. Excellent communication and delivery. Will update if product is anything but excellent.	1 day
5 of 5	Excellent service and shipping! Thank you very much.	1 day
5 of 5	YESSSS!!! ORDER FROM THIS VENDOR!! This ketamine is amazing. Packaging/stealth was dead on 5/5 A+++. Even if the package was opened there's little chance that anyone would be messing with the contents.	
5 of 5	Now as the the actual package's contents… 5/5!! HOLY SHIT! It's the largest crystals Ive ever seen in a K package before. I crushed the smallest amount yesterday and was feeling great. I can't wait to have a full blown experience on this extraordinarily clean product. HIGHLY RECOMMENDED VENDOR!!	2 days
5 of 5	Just in time for the weekend :)	2 days
5 of 5	Wish I could give 6/5. Seller went above and beyond what a retail store would. Answered questions promptly, shipped within 24 hours, recieved 3 days from time of order. Excellent stealth! Product was just as described receieved in one shard :) Will be ordering again.	2 days

Figure 1. Review page from *Silk Road* website (accessed 25 November 2013).

record of illicit transaction conducted online, authorities who intercept a consignment with a false name and address are left unable to verify those parties for whom the drugs are intended.

In circumstances such as these, policing agencies may seek to take additional measures to confirm the identity of suspected buyers. These could include placing recipient addresses under surveillance; cameras could covertly monitor a pick-up point or, even better, be installed inside a recipient address so as to capture footage of suspects opening drug consignments and inspecting the goods inside. With this kind of footage, gaining sufficient evidence to justify a charge and secure a conviction is more feasible. Importantly, however, the costs and benefits associated with this kind of invasive and expensive operation are likely to be significantly unbalanced. As noted earlier, most transactions conducted via *Silk Road* are for purchases of relatively small amounts of illicit drugs. This means that the volume of drugs which most buyers receive is relatively

22-11-2012: IMPORTANT NOTICE FOR AUSTRALIAN CUSTOMERS ONLY!:
We are reconsidering how to handle shipments to Australia, this because we noticed the past week more and more are not getting through. It's no surprise everybody knows on the road what extra complications shipping from Europe to Australia brings along. No other border security is so obsessive on checking the mail. We have had good results but it looks like there is much more control going on and next to that Australian customers are flaming us on the forum while they know ordering for them is more of danger. We can't allow this too hurt us on the longer term…

We had to think of what to do, and came up with a changed resolution policy for Australians…
NORMAL REFUND POLICY:
Up to $1500 orders: 50% refund or 100% reship
Above $1500 orders by un-tracked no need to sign shipping method: 30% refund
Above $1500 orders by tracked shipping needs to sign shipping method: = 50% refund

AUSTRALIAN REFUND POLICY:
This policy is only for Australian customers. Australia is a tough country to ship to as a buyer you should keep this mind when ordering there is just more chance of failure than to any other country in the world. When ordering you accept the following terms:
* NO RESHIPPING
* 30% REFUND

Figure 2. Seller page from *Silk Road* website (accessed 25 November 2013).

small and (depending on jurisdiction) would likely constitute a lower-level drug possession rather than commercial trafficking charge.

Expending scarce police resources on low-level drug offences may be easier to justify when buyers can at least be compelled to provide evidence as to the identity of their supplier. However, unlike 'in-person' drug exchanges, with transactions conducted via *Silk Road*, this information is at no stage available to buyers, who only have access to the most limited (and, from their perspective, the most relevant) information as to whom they are purchasing from: the seller's cryptonym, the types and prices of available goods, the countries to which goods can be sent and any user satisfaction ratings or comments. As buyers have no further information about the identity of sellers, any successful prosecution of an offender can only result in a dead end: the conviction of an end-user with no possibility of following on to more serious links in the chain of supply.

Long-term challenges

Using *Silk Road* is clearly not without risk. Buyers and sellers may be lazy or complacent and fail to conceal adequately their goods or protect their online anonymity; they may engage in risky dealing methods to 'sell on' goods purchased online; or they may simply be unlucky and fall foul of random or unexpectedly rigorous inspections. Individuals using the site therefore remain vulnerable to law enforcement agencies that are

sufficiently well resourced and determined to secure a conviction. However, while the complex challenges currently facing law enforcement will not entirely prevent them from securing convictions for offences committed via the site, they do point to significant longer-term difficulties in enforcing drug prohibition.

One particularly complex strategic challenge facing law enforcement is that of resource allocation. As with any organization, police forces and customs agencies are forced to make decisions about where best to allocate resources so as to yield maximum results. To this end, domestic anti-narcotics operations have traditionally been allocated towards either 'high-end' policing, which targets the importers/distributors located at the middle echelons in the chain of supply, or lower-level or 'retail' enforcement that targets street dealers and end-users in known drug hot-spots (Benavie, 2009). Neither of these strategies is likely to have a significant impact on *Silk Road* distribution networks which run directly between drug manufacturers/cultivators to consumers. These new distribution networks bypass conventional drug importers, as well as middle- and lower-level dealers, meaning that (from the perspective of *Silk Road* users, at least) these targets of law enforcement are no longer relevant. Rather than targeting middle links in the chain of supply, the only other option available to domestic investigators is to target end-users whose orders are intercepted while in transit. End-users obtaining drugs via *Silk Road* are less vulnerable to conventional anti-narcotics operations such as raids on known drug hot-spots. This is because *Silk Road* users have their orders delivered directly to their home (or an alternative address), meaning that there is no requirement to frequent areas known by the police for their association with drug dealing.

Despite rhetoric to the contrary, drug prohibition regimes are overwhelmingly targeted towards end-users. In the United States, for example, more than 80 per cent of drug-related arrests are for simple possession rather than trafficking, sale or manufacture (FBI, 2013). However, there are important symbolic reasons necessitating that law enforcement also continue to target higher-level suppliers. The arrest of these elusive parties provides important symbolic and public relations opportunities. As is so often presented in the media, big busts regularly result in a press conference where a table is stacked high with dangerous drugs and small arms (and preferably accompanied by tattooed and angrily defiant foreign gangsters). These clichéd images – large quantities of drugs and guns, and human symbols of foreign threat/corruption – are the stock-standard and archetypal representations of War on Drugs propaganda (Boyd, 2008).

Images that link illicit drugs with violence and organized crime are vital in maintaining public support for drug prohibition, a fact reflected in their ongoing popularity and use by law enforcement. Unfortunately for those concerned with maintaining the visual link between drugs, violence and organized crime, none of these images can easily be associated with the operations of *Silk Road*. Online drug sellers who communicate openly with their clients, who are sensitive to consumer needs and offer refunds for intercepted drugs, and who even engage in traditional marketing gimmicks such as Halloween and Christmas discount specials, contrast markedly with stereotypical representations of dope dealers as predatory psychopaths and stone-cold killers (see Boyd, 2008; Cohen, 2006). So too do representations of the hopeless or crazed 'junkie' jar significantly with the prosaic blandness of online shoppers and user discussion forums complaining about minor delays in shipping. It is this very lack of drama that threatens to undermine the

efficacy and credibility of violent, anti-drugs propaganda. Without large individual shipments of narcotics, and in the absence of guns, gangsters and turf wars, proponents of the War on Drugs are left without some of their most potent symbolic devices (Boyd, 2008).

Potential Impacts on Drug Distribution Networks

Contemporary research points to the dominance of networks in the distribution of various illicit drugs. From Colombian cocaine (Kenney, 2007), to Australian methamphetamine (Bright et al., 2012), to heroin in New York (Natarajan, 2006), there is a growing view among scholars that decentralized networks now supply the bulk of various drug markets (see also Dorn et al., 1992; Heber, 2009; Malm and Bichler, 2011; Moreselli, 2009; Morselli and Petit, 2007; Natarajan and Hough, 2000). This is in stark contrast to earlier models of distribution, whereby centralized and hierarchical organized crime groups were believed (often erroneously) to have played this central role (Edwards and Levi, 2008; Kenney, 2007). Commercial distribution networks, particularly those centred on illicit drugs, are dynamic and highly variable, and determining their composition beyond a conceptual stage is complicated by a range of factors. These include the different production and consumption patterns associated with each drug; the limited time each participant stays connected to the network; and the covert nature of illicit markets in general, where even those closely involved may be unaware of the number or nature of other distributors beyond their immediate range of contacts (Pearson and Hobbs, 2001).

Despite the elusiveness and variability inherent to drug distribution networks, a number of common features may still be determined. At a fundamental level, all networks are composed of various interconnected nodes. These necessarily involve both producers and consumers who are usually connected through an array of intermediaries. At their most basic, drug distribution networks are small and simple, as is the case when narcotic plants (e.g. opium poppies or marijuana) are grown at home, or when clandestine manufacturing labs are set up by users to create illicit drugs for their own personal use or for that of acquaintances. In these cases, the entire network may comprise only a few individuals. Alternatively, drug distribution networks may be large and complex, and involve multiple and shifting layers of domestic and international manufacturers, traffickers, brokers, wholesalers and street-level retailers. In these large and decentralized networks, individual nodes may come and go without affecting the overall integrity of the system. If a node is eliminated – for instance through arrest or violence at the hands of a competitor – then distribution is simply rerouted through adjacent nodes. The flexibility inherent to networked systems explains their characteristic durability, and accounts for the continued functioning of illicit drug networks despite the ongoing removal of dealers, traffickers or any other nodes that constitute part of the system of distribution (Bright et al., 2012; Malm and Bichler, 2011; Morselli and Petit, 2007).

The advantages of decentralized and networked distribution do, however, come with significant costs. Complex networks with large numbers of intermediary nodes carry inefficiencies that affect the price and purity of distributed drugs. This is because commercial distribution networks rely on financial incentives to compensate individual nodes for their involvement. Financial compensation can be achieved

through the imposition of incremental price increases at each point of transaction; these can then be retained by each node as profit. The higher the overall number of nodes that are involved with distribution, the greater the financial impost on the final retail price of the purchased drug. This practice explains the significantly higher prices of drugs at the street level when compared to the same quantity of product at the wholesale or trafficking stages (Pearson and Hobbs, 2001). An alternative to simply increasing the price of a drug is to adulterate or 'cut' the product. This involves diluting the drug with a cheaper substance so as to increase the overall quantity that can be sold at the same, or an even a higher price. Product adulteration allows distributing nodes another opportunity to attain a share of profit, and accounts for how illicit drugs may decrease in purity between the production and retail stages of distribution.

In this context, the significance of *Silk Road* becomes apparent when considering the capacity for distribution links to form directly between producers and consumers. Under a direct distribution model, there is no necessity for the involvement of drug traffickers, brokers, wholesalers, street retailers or other intermediary nodes. Drugs can simply be posted directly from producers to consumers (both domestically and internationally), who can find each other literally at the click of a button. Unlike alternative systems of distribution (see, for example, Dorn et al., 1992) there is no necessity for personal interaction or any other contact between parties. The ease with which these direct distribution links may be formed has significant implications, particularly for various intermediary nodes who may find themselves cut out of the distribution network entirely. By contrast, the consequences of more direct distribution are likely to be beneficial for drug consumers. The reduced number of nodes involved means more efficient operation of the network, resulting in fewer price increases and, less necessity for product adulteration. This means that consumers are able to source better quality products, and at a lower price, than those available from street retailers. Christin's (2012) research into *Silk Road* indicates just this: extraordinarily high levels of consumer satisfaction regarding the price and purity of drugs purchased online.

Care needs to be taken to not overstate the transformational potential of direct online drug distribution. One significant limitation is that online distribution is only possible where sufficient communications infrastructure is available to facilitate links between buyers and sellers. In regions where one or both of these ends of the distribution network are unable to connect online, intermediary nodes will remain essential. For example, peasant coca farmers in Latin America, or Afghani villagers harvesting raw opium may not have sufficient access to the internet technologies and secure postal networks required to conduct exchanges via *Silk Road*, and may therefore only be able connect to broader distribution networks through intermediaries. This indicates that online communications and cryptomarket technologies are not yet capable of eliminating completely the involvement of intermediary nodes across the world's various drugs markets. More research is necessary to determine how various drug markets will respond to technological changes in this area.

Online drug distribution presently accounts for a small, but steadily growing share of the global trade in illicit drugs (Christin, 2012). As this proportion continues to expand, various drug markets will adapt in different ways. Regardless of their

composition, however, online communications and cryptomarket technologies have significant potential to reduce the size and complexity of distribution networks as more direct links increasingly are formed between producers and consumers. These developments suggest that while law enforcement may face serious challenges from the emergence of *Silk Road* and other cryptomarkets, the real losers from the growth of online distribution will be the drug traffickers, street dealers and other intermediary nodes who may find themselves superfluous to a less complex and more efficient system of illicit exchange.

Conclusion

It is tempting to frame the development of *Silk Road* purely in terms of the challenges the site poses to law enforcement and contemporary drug prohibition. However, *Silk Road* also provides a striking example of how developments in online technology produce transformational change in the illicit as well as licit economies. Just as legitimate online retailers have transformed conventional global and domestic marketplaces, so too does *Silk Road* have the potential to wreak similar havoc among traditional drug distribution networks. The long-term implications of these changes have important implications for the global drugs industry. More direct online distribution networks between drug producers and consumers may significantly curtail the involvement of narco-traffickers and street-level gangs in global and domestic drug distribution. Cryptomarket technology – of which *Silk Road* is just the largest iteration – therefore presents one of the most promising opportunities to remove much of the violence associated with illicit drugs (while also offering cheaper, higher quality products to drug consumers). Law enforcement and state authorities should be mindful of these broader benefits to society when considering how best to respond to *Silk Road* as well as to other cryptomarkets which have the potential to transform a vast global industry currently blighted by appalling levels of incarceration and violence.

This article has argued that the operations of *Silk Road* may be interpreted as a less harmful alternative than those currently offered by the conventional illicit drug economy. However, the rise of cryptomarkets more generally presents a much more ambivalent picture. While the potential of *Silk Road* to minimize the violence associated with illicit drug distribution may become evident as the site continues to grow, it is difficult to perceive any broader social benefit offered by other cryptomarkets which deal in explicitly malicious goods or services, such as stolen credit cards, child pornography or contract killing. The threats posed by the rapid proliferation of these sites are largely unknown. It is therefore a task of no small priority for criminologists to conduct further research into cryptomarkets, and shine a light into the deeper recesses of the dark net.

Acknowledgements

The author would like to thank Jude McCulloch, Dean Wilson, Julian Droogan and Chris Blain, as well as the two anonymous reviewers, for their insights and significant contributions to the article.

Notes

1. TOR – an acronym for *The Onion Router* – is a 'circuit-based low-latency anonymous communication service' (Dingledine et al., 2004: 1) developed in collaboration with US military intelligence and launched in 2004. For more information see Dingledine et al. (2004).
2. Naturally, inspecting international post is only relevant for those exchanges that are conducted across state borders; much of the traffic sent through *Silk Road* is intended for domestic consumption only, and items sent through the domestic post are not subject to particular scrutiny from either Customs agencies or police.

References

Australian Federal Police (AFP) (2012) AFP and Customs warn users of Silk Road. AFP website, available at: http://www.afp.gov.au/media-centre/news/afp/2012/july/afp-and-Customs-warn-users-of-silk-road.aspx (accessed 20 February 2013).

Barratt M (2012) Letters to the editor: 'Silk Road: Ebay for drugs'. *Addiction* 107: 683–684.

Barratt M, Lenton S and Allen M (2013) Internet content regulation, public drug websites and the growth in hidden internet services. *Drugs: Education, Prevention and Policy* 20(3): 195–202.

Benavie A (2009) *Drugs: America's Holy War*. New York: Routledge.

Blain L (2013) 300 million dollars out of thin air. Gizmag website, available at: http://www.gizmag.com/bitcoin-creation-value-overview/26325/ (accessed 3 March 2013).

Boyd S (2008) *Hooked: Drug War Films in Britain, Canada and the United States*. New York: Routledge.

Bright D, Hughes C and Chalmers J (2012) Illuminating dark networks: A social network analysis of an Australian drug trafficking syndicate. *Crime, Law and Social Change* 57: 151–176.

Chen A (2011) The underground website where you can buy any drug imaginable. *Gawker*, available at: http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable (accessed 9 September 2011).

Christin N (2012) Travelling the *Silk Road*: A measurement analysis of a large anonymous online marketplace. Working Paper, Carnegie Mellon.

Cohen M (2006) Jim Crow's drug war: Race, Coca Cola, and the Southern origins of drug prohibition. *Southern Cultures* 12(3): 55–79.

Dingledine R, Mathewson N and Syverson P (2004) *Tor: The Second-Generation Onion Router*. Washington, DC: US Naval Research Lab.

Dorn N, Murji K and South N (1992) *Traffick: Drug Markets and Law Enforcement*. London: Routledge.

Duffy C (2012) Dealers shed light on dark internet's drug trade. ABC News website, available at: http://www.abc.net.au/news/2012-12-05/dark-internet-linked-to-drug-seizure-spike/4410872 (accessed 12 September 2013).

Edwards A and Levi M (2008) Researching the organisation of serious crimes. *Criminology and Criminal Justice* 8: 363–388.

Federal Bureau of Investigation (FBI) (2013) Crime in the United States: 2011. FBI website, available at: http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2011/crime-in-the-u.s.-2011/persons-arrested/persons-arrested (accessed 1 February 2013).

Greenblat E (2011) Post unpacks parcel boom, but it's a mixed bag. *The Age*, available at: http://www.theage.com.au/national/post-unpacks-parcel-boom-but-its-a-mixed-bag-20110919-1khzh.html (accessed 5 December 2012).

Hammersly B (2012) *64 Things You Need to Know Now for Then: How to Face the Digital Future without Fear*. Google eBook.

Heber A (2009) The networks of drug offenders. *Trends in Organised Crime* 12: 1–20.

Jewkes Y and Yar M (2010) The internet, cybercrime and the challenges of the twenty-first century. In: Jewkes Y and Yar M (eds) *Handbook of Internet Crime*. Devon: Willan Publishing.

Kenney M (2007) The architecture of drug trafficking: Network forms of organisation in the Colombian cocaine trade. *Global Crime* 8(3): 233–259.

Malm A and Bichler G (2011) Networks of collaborating criminals: Assessing the structural vulnerability of drug markets. *Journal of Research in Crime and Delinquency* 48: 271–297.

Morselli C (2009) *Inside Criminal Networks*. New York: Springer.

Morselli C and Petit K (2007) Law-enforcement disruption of a drug importation network. *Global Crime* 8(2): 109–130.

Moses A (2012) 'Dark net' drug deals boom on cyber *Silk Road*. *Sydney Morning Herald*, available at: http://www.smh.com.au/technology/technology-news/dark-net-drug-deals-boom-on-cyber-silk-road-20120809-23wdj.html#ixzz2680dVGK5 (accessed 11 September 2012).

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. Bitcoin website, available at: http://bitcoin.org/bitcoin.pdf (accessed 20 February 2013).

Natarajan M (2006) Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. *Journal of Quantitative Criminology* 22: 171–192.

Natarajan M and Hough J (2000) *Illegal Drug Markets: From Research to Prevention Policy*. New York: Criminal Justice Press.

Ormsby E (2012) The drug's in the mail. *The Age*, available at: http://www.theage.com.au/victoria/the-drugs-in-the-mail-20120426-1xnth.html (accessed 12 September 2012).

Pauli D (2012) Aussie coppers bedevilled by online contraband networks. *SC Magazine*, available at: http://www.scmagazine.com.au/Tools/Print.aspx?CIID=314984 (accessed 11 September 2012).

Pearson G and Hobbs D (2001) *Middle Market Drug Distribution*. Home Office Research Study no. 224. London: Home Office.

Ruggerio V (2000) *Crime and Markets: Essays in Anti-Criminology*. Oxford: Oxford University Press.

Schneider J (2003) Hiding in plain sight: An exploration of the illegal(?) activities of a drugs newsgroup. *Howard Journal of Criminal Justice* 42(4): 374–389.

United Nations Office on Drugs and Crime (UNODC) (2005) *World Drugs Report*. Vienna: UNODC.

Van Hout M and Bingham T (2013) Silk Road, the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy*, available at: http://dx.doi.org/10.1016/j.drugpo.2013.01.005.

Wall D (2007) *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Author biography

James Martin is a Senior Lecturer at the Macquarie University Centre for Policing, Intelligence and Counter-terrorism. His current research interests include *Silk Road* and online drug distribution, the global War on Drugs, cybercrime and policing.